STUDIA IURIDICA TORUNIENSIA
TOM VI

Aleksandra Kiedrowicz-Wywiał

Oszustwo komputerowe w polskim i niemieckim kodeksie karnym

Przestępstwo oszustwa komputerowego jest młodą regulacją, wprowadzoną do polskiego kodeksu karnego w 1997 roku, wraz z szeregiem innych przestępstw komputerowych[1]. Było to spowodowane szybkim rozwojem informatyzacji życia oraz przestępczości komputerowej, wymuszających na ustawodawcy konkretne działania. Pojawienie się tego nowego typu przestępstwa w polskim porządku prawnym zostało poprzedzone raportami i propozycjami organizacji międzynarodowych jak również doświadczeniami innych państw. Oszustwo komputerowe zostało bardzo wcześnie spenalizowane w Niemczech i to ten kraj miał bardzo duży wpływ na kształt rozwiązań modelowych. W konsekwencji regulacja polska wykazuje wiele cech wspólnych z niemiecką.

Geneza regulacji przestępstwa oszustwa komputerowego

Do 1986 roku niemiecki kodek karny (*Strafgesetzbuch* – w skrócie StGB) przewidywał jedynie regulację tradycyjnej formy oszustwa w § 263[2]. Pierwszy raz konieczność zmiany lub wprowadzenia nowej

[1] Dz.U. z 1997 r. Nr 88, poz. 553.

[2] „Kto w celu osiągnięcia bezprawnej korzyści majątkowej dla siebie lub dla kogoś innego doprowadza do powstania szkody majątkowej w mieniu

formy tego przepisu dostrzeżono już w latach siedemdziesiątych. Przyczyny takiego stanu rzeczy autorzy niemieccy[3] upatrują w wyroku w sprawie kart płatniczych, który zapadł 26 czerwca 1972 roku. Skład drugiej izby karnej Sądu Federalnego orzekł w nim, że nadużycia związane z kartami czekowymi nie wypełniają znamion przestępstwa nadużycia zaufania (§ 266 StGB), lecz oszustwa. Tok swego rozumowania Sąd oparł na fakcie, że do zaistnienia przestępstwa określonego w § 266 StGB konieczne jest, aby na sprawcy spoczywał szczególny obowiązek pieczy nad majątkiem poszkodowanego. Przy zawieraniu umowy rachunku bankowego bank zobowiązuje się dbać o interesy swojego klienta. Nie ma jednak miejsca sytuacja odwrotna. Tak więc w przypadku nadużycia karty przez jej uprawnionego posiadacza można jedynie rozważać zastosowanie regulacji oszustwa (§ 263 StGB). Tę linię orzeczniczą potwierdził następnie wyrok z 13 czerwca 1985 roku – tzw. rozstrzygnięcie w sprawie kart kredytowych. W tej sprawie sąd uściślił jednak, że mowa o oszustwie może być tylko w przypadku, gdy klient wprowadzi bank w błąd co do faktu swojej uprzedniej karalności, danych osobowych lub ważności samej karty. Jednak użycie karty w sytuacji, gdy jest ona bez pokrycia, nie wypełni znamion przestępstwa określonego w § 263 StGB. Podsumowując, w Niemczech od lat siedemdziesiątych aż do 1986 roku szereg nadużyć związanych z użyciem kart kredytowych nie było penalizowanych. W kontekście tych wydarzeń, po długotrwałych pracach legislacyjnych, 15 maja 1986 roku uchwalono drugą ustawę o zwalczaniu przestępczości gospodarczej. Weszła ona w życie 1 sierpnia 1986 roku.

W uzasadnieniu projektu ustawy wskazywano przede wszystkim na potrzebę zlikwidowania istniejącej w systemie karnym luki, co

---

innej osoby przez to, że wprowadza ją w błąd lub utrzymuje w błędzie poprzez przedstawienie fałszywych faktów lub wypaczanie albo zatajanie prawdziwych faktów, podlega karze pozbawienia wolności do lat pięciu lub karze grzywny".

[3] Por. H. Scheffler, *Das 2. Gesetz zur Bekämpfung der Wirtschaftskriminalität unter besonderer Berücksichtigung des Tatbestandes des Computerbetruges (§ 263a StGB) und des Tatbestandes des Missbrauchs von Scheck – und Kreditkarten (§ 266b StGB)*, Kiel 1998; H. Otto, *Probleme des Computerbetrugs*, Jura 1993, z. 11.

miało być kontynuacją rozpoczętej już wcześniej reformy prawa karnego. Jednocześnie podkreślano, że nowelizacja nie ma być przeprowadzona poprzez zmianę lub uzupełnienie znamion penalizowanych już zachowań, ale przez wprowadzenie nowych, uzupełniających regulacji[4]. Tym samym odrzucono wzorowaną na prawodawstwie amerykańskim koncepcję wprowadzenia penalizacji tzw. nadużycia komputerowego, które miałoby regulować wyczerpująco zarówno nieupoważnione użycie komputera, jak i nieupoważnione zapoznanie się z danymi oraz wtargnięcie do systemu automatycznie przetwarzającego dane[5]. W związku z powyższym konstrukcja regulacji oszustwa komputerowego została oparta w znacznej mierze na znamionach przestępstwa oszustwa klasycznego i umieszczona w kodeksie zaraz za nim jako § 263a.

Reforma niemieckiego prawa karnego była jedną z pierwszych na świecie prób wzmocnienia prawnokarnej ochrony przed przestępczością komputerową. Poprzedziły ją legislacje szwedzka (1973), brytyjska (1981) i stanowe w ok. 20 stanach Stanów Zjednoczonych (w latach 1978–1984)[6].

Pierwsze działania na płaszczyźnie międzynarodowej, mające na celu harmonizację prawa karnego w dziedzinie przestępczości komputerowej, zostały podjęte przez Organizację Współpracy i Rozwoju Ekonomicznego w Europie (Organisation for Economic Cooperation and Development – OECD). W ich wyniku powstał raport[7] zawierający analizę ówczesnych regulacji prawnych państw członkowskich, odmienności między penalizacją przestępstw „tradycyjnych" a tych związanych z nowymi technologiami oraz propozycje dalszych działań legislacyjnych. Na liście minimalnej czynów, które powinny być penalizowane, znalazło się m.in. przestępstwo oszustwa kompute-

---

[4] H. Otto, op.cit., s. 612.

[5] S. Frey, *Computercriminalität in eigenturms – und vermögensstraflicher Sicht*, Florentz–München 1987, s. 173.

[6] Ibidem, s. 173.

[7] *Computer-related crime: analysis of legal policy*, Organisation for Economic Co-operation and Development, Paryż 1986. W tworzeniu raportu aktywny udział brały Niemcy – w państwie tym od 1974 r. prowadzony jest rejestr spraw karnych związanych z wykorzystaniem nowoczesnej technologii, co znacznie ułatwiło prace.

rowego (czyli wprowadzenie, zmiana, usunięcie i/lub zablokowanie danych i/lub programów komputerowych, które jest popełniane umyślnie z zamiarem dokonania nielegalnego transferu środków finansowych lub innych przedmiotów wartościowych[8]).

Rozwój technologii informatycznych nie pozostał również bez wpływu na prace Rady Europy. Pierwsze rezolucje dotyczyły ochrony danych osobowych[9]. Dopiero w 1985 roku obrady rozpoczęła komisja ekspertów do spraw przestępczości komputerowej i sytuacja ta uległa zmianie. Wynikiem prac komisji był projekt zalecenia dotyczący przestępstw związanych z użyciem komputera. Dokument ten, przyjęty w 1989 roku, zawierał wskazania legislacyjne dla rządów krajów członkowskich dotyczące zmian ustawodawczych i zakresu kryminalizacji działań przestępczych z zakresu przestępczości komputerowej. Zalecenia te zostały ujęte w na dwóch listach – na „liście minimalnej" (czyny, dla których zwalczania zdaniem komisji konieczna jest wspólna polityka kryminalna państw członkowskich i które tym samym powinny być penalizowane) oraz na „liście opcjonalnej". Również w tym przypadku przestępstwo oszustwa komputerowego (*computer fraud*) zostało uznane za duże zagrożenie i tym samym znalazło się na liście minimalnej[10]. Zdefiniowano je jako wprowadzenie, zmianę, usunięcie lub zablokowanie danych lub programów komputerowych, lub zakłócenie procesu przetwarzania danych, które wpływa na wynik przetwarzania danych, tym samym powodując szkodę majątkową innej osobie,

---

[8] „[…] the input, alteration, erasure and/or suppression of computer data and/or computer programs made willfully with the intend to commit an illegal transfer of funds or of another thing of value", ibidem, s. 641.

[9] Rezolucja nr (73)22, rezolucja nr (74)29 i Konwencja o ochronie osób w związku z automatycznym przetwarzaniem danych o charakterze osobowym z 1981 r.

[10] Prócz tego inne czyny przestępcze to: fałszerstwo komputerowe (*computer forgery*), uszkodzenie danych lub programu komputerowego (*damage to computer data or computer programs*), sabotaż komputerowy (*computer sabotage*), nieuprawniony dostęp, przechwycenie, nieuprawnione odtworzenie chronionego programu komputerowego lub topografii układu scalonego (*unauthorized access*, *interception*, *unauthorised reproduction of a protected computer program*, *topography*).

z zamiarem bezprawnego osiągnięcia korzyści majątkowej dla siebie lub dla innej osoby[11].

W związku z szybkim rozwojem nowych technologii, a przede wszystkim wzrastającymi możliwościami przesyłu danych, przyjęcie rekomendacji (89)9 okazało się niewystarczające. Niwelowanie różnic między systemami prawnymi państw członkowskich nie zapewniało już skutecznej obrony przeciwko wzrastającemu zagrożeniu ze strony cyberprzestępczości. Dlatego Komitet Problemów Przestępczości Rady Europy powołał w 1996 roku Komitet ds. Przestępstw Popełnianych w Cyberprzestrzeni. W wyniku prac Komitetu 23 listopada 2001 roku otwarto do podpisu konwencję dotyczącą przestępstw popełnianych w sieciach komputerowych[12], która weszła w życie 1 lipca 2004 roku. Regulacja ta zawiera listę przestępstw komputerowych, wskazania dotyczące karalności form stadialnych i zjawiskowych, zasadę odpowiedzialności karnej osób prawnych za przestępstwa konwencyjne, zasady jurysdykcji transgranicznych przestępstw komputerowych oraz przesłanki ekstradycji ich sprawców, a także postanowienia dotyczące zagadnień procesowych[13]. Konwencja wskazuje na pewne standardy minimalne penalizacji określonych zachowań, które jednak państwa członkowskie mogą dobrowolnie rozszerzać. Autorzy podzielili penalizowane zachowania na cztery grupy[14], zaliczając oszustwo komputerowe wraz z fałszerstwem komputerowym do kategorii prze-

---

[11] „The input, alteration, erasure or suppression of computer data or computer programs, or other interference with the course of data processing, that influences the result of data processing thereby causing economic or possessory loss of property of another person with the intent of procuring an unlawful economic gin for himself or for another person". Propozycja alternatywna: w zamiarze bezprawnego pozbawienia mienia innej osoby – „with the intent to unlawfully deprive that person of his property". U. Sieber, *The International Emergence of Criminal Information Law*, Köln–Berlin–Bonn–München 1992, s. 78–79.

[12] Convention on Cybercrime, CETS, No. 185.

[13] Por. A. Adamski, *Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu konwencji Rady Europy*, Toruń 2001, s. 10.

[14] Przestępstwa przeciwko poufności, integralności i dostępności danych i systemów komputerowych, przestępstwa związane z użyciem komputera,

stępstw związanych z użyciem komputera. Zostało ono zdefiniowane w art. 8 jako umyślne spowodowanie utraty własności przez inną osobę na skutek wprowadzenia, zmiany, usunięcia lub zablokowania danych informatycznych albo innej ingerencji w funkcjonowanie systemu informatycznego w zamiarze przysporzenia sobie lub innej osobie bezprawnej korzyści majątkowej.

Polska podpisała Konwencję 23 listopada 2001 roku. Nie została ona jednak jeszcze ratyfikowana.

Konstrukcja art. 287 k.k. i § 263a StGB

Czynności wykonawcze

Odmiany czynności wykonawczych są w art. 287 k.k. wyliczone taksatywnie i należą do nich: wpływanie na automatyczne przetwarzanie danych informatycznych, wpływanie na automatyczne gromadzenie danych informatycznych, wpływanie na automatyczne przekazywanie danych informatycznych, zmienianie danych informatycznych, usuwanie danych informatycznych oraz wprowadzanie nowego zapisu danych informatycznych. Natomiast niemiecki ustawodawca w § 263a StGB jako znamiona przestępstwa oszustwa komputerowego wymienia: wpływanie na rezultat procesu przetwarzania danych poprzez niewłaściwe ustawienie programu, wprowadzenie niewłaściwych lub niepełnych danych, nieuprawnione użycie (zastosowanie) danych lub jakiekolwiek inne nieuprawnione oddziaływanie na proces przetwarzania danych[15]. Mimo że regulacje te

przestępstwa komputerowe ze względu na charakter informacji stanowiącej ich przedmiot oraz przestępstwa przeciwko własności intelektualnej – ibidem, s. 17.

[15] „Wer in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt, dass er das Ergebnis eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf beeinflusst, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft".

zostały sformułowane nieco odmiennie, to można stwierdzić, iż ich zakres penalizacji praktycznie się pokrywa. W porównaniu z „tradycyjnym" oszustwem znamiona art. 287 k.k. i § 263a StGB zostały zakreślone bardzo szeroko. Wydaje się to zrozumiałe – intencją ustawodawcy było uregulowanie zjawisk będących wynikiem rozwoju nowoczesnych technologii. Im szerszy więc zakres odpowiedzialności określony w przepisie, tym większe prawdopodobieństwo, że regulacja ta nie straci w najbliższym czasie na aktualności w wyniku dalszego postępu technicznego[16]. Z drugiej strony pojawiły się obawy, że ten bądź co bądź świadomy zabieg ustawodawcy może doprowadzić do stanu nieokreśloności zasad odpowiedzialności karnej. Tym samym przepisy te musiałyby zostać uznane za niekonstytucyjne. Jednak mimo wątpliwości wyrażanych w doktrynie zarówno niemieckiej[17], jak i polskiej[18] konstytucyjność tych regulacji nie została jak dotąd zakwestionowana.

Oszustwo komputerowe, a oszustwo „klasyczne"

W tym miejscu nasuwa się pytanie, dlaczego ustawodawca, zamiast tworzyć całkiem nową regulację, nie uzupełnił przepisu § 263 o nowe znamiona, dzięki czemu zakres penalizacji przestępstwa oszustwa „klasycznego" obejmowałby również zjawiska związane z automatycznym przetwarzaniem danych. Takie propozycje były wysuwane w trakcie obrad komisji ekspertów do spraw zwalczania przestępczości gospodarczej (Lenckner, Sieber, Haft). Zabieg dodania nowego akapitu do już istniejącego § 263 StGB miałby zapobiec wątpliwościom interpretacyjnym przez ścisłe powiązanie znamion oszustwa komputerowego i oszustwa „klasycznego"[19]. Jak

---

[16] P. Kardas, *Oszustwo komputerowe w kodeksie karnym*, Przegląd Sądowy 2000, z. 11–12, s. 57; R. Korczyński, R. Koszut, *„Oszustwo" komputerowe*, Prokuratura i Prawo 2002, z. 2, s. 26.

[17] E. Schlüchter, *Zweites Gesetz zur Bekämpfung der Wirtschaftskriminalität*, Heidelberg 1987, s. 91.

[18] P. Kardas, op.cit., s. 57; R. Korczyński, R. Koszut, op.cit., s. 26.

[19] S. Frey, op.cit., s. 183.

zauważa S. Frey, utworzenie typu szczególnego przestępstwa oszustwa miałoby tę zaletę, że nie powstawałyby żadne wątpliwości, iż oszustwo komputerowe sprowadza się do zamachu na mienie, tyle tylko, że przy pomocy nowych środków. Nie chodzi tu więc o zamach na nowe dobro, dotychczas niechronione prawem[20]. W trakcie prac kodyfikacyjnych podjęto jednak decyzję o ujęciu tej regulacji w oddzielnym paragrafie, gdyż istnienie typu szczególnego oszustwa penalizującego zachowania oszustów komputerowych miałoby wywołać w społeczeństwie wrażenie, że nie są oni oszustami pospolitymi. Zamiast tego mieliby być postrzegani jako „lepsi" sprawcy, korzystający z techniki niezrozumiałej dla większości społeczeństwa i przez to nie odpowiadaliby tradycyjnemu obrazowi przestępcy[21]. Jednak wątpliwości odnośnie do relacji między art. 286 a art. 287 k.k. oraz § 263 a § 263a StGB pojawiają się (np. próby wykładni § 263a w powiązaniu z § 263 StGB[22], niejasne dla praktyków rozróżnienie między czynami penalizowanymi na gruncie art. 286 a art. 287 k.k.[23]). Geneza regulacji oszustwa komputerowego, jej umieszczenie w bezpośrednim sąsiedztwie artykułu penalizującego zwykłe oszustwo, a w przypadku ustawy niemieckiej – ukształtowanie znamion na podobieństwo przepisu § 263 StGB – wszystko to sprawia, że stosunek regulacji przestępstwa oszustwa komputerowego do regulacji oszustwa „klasycznego" nie jest jasny. W konsekwencji w literaturze i w orzecznictwie niemieckim można spotkać się z dwiema metodami wykładni przepisu § 263a StGB, autonomiczną i związaną. Wykładnia autonomiczna polega na interpretacji niepowiązanej z elementami charakterystycznymi dla przestępstwa oszustwa „klasycznego". Natomiast metoda wykładni związanej (*betrugsnahe Auslegung*) odnosi się do jego charakterystyki normatywnej[24]. Tutaj wskazuje się, że przepis regulujący oszustwo komputerowe ma na celu jedynie zlikwidowanie luk

---

[20] Ibidem, s. 183.

[21] Ibidem, s. 184.

[22] P. Kardas, op.cit., s. 55, S. Frey, op.cit., s. 182.

[23] A. Adamski, *Oszustwo komputerowe a oszustwo internetowe*, [w:] *Przestępczość teleinformatyczna*, red. J. Kosiński, Szczytno 2005, s. 15.

[24] P. Kardas, op.cit., s. 55.

w prawodawstwie, które powodują, że przepis § 263 StGB często nie obejmuje penalizacją działań oszukańczych, do których używane są komputery. Takie oparcie się w toku wykładni na regulacji przestępstwa oszustwa ma być zabezpieczeniem przed tym, aby nowa norma nie była w swoim działaniu regulacją dalej idącą[25]. Wykładnia związana opiera się na spostrzeżeniu, że chociaż w ciągu wielu lat istnienia regulacji przestępstwa oszustwa obrosło ono komentarzami doktryny kładącymi nacisk przede wszystkim na ludzkie procesy postrzegania i kształtowania woli, to samą istotę działania oszukańczego, tj. zamach na mienie, posłużenie się materialną nieprawdą, można nadal odnaleźć w konstrukcji oszustwa komputerowego[26]. Nowe są jedynie środki, dzięki którym sprawca dokonuje zamachu. Przedstawiciele tego nurtu borykają się jednak z problemem, jak pogodzić regulację dostosowaną do relacji człowiek–człowiek z rzeczywistością, w której zachodzi interakcja na linii człowiek–maszyna. Szczególnie wiele wątpliwości wywołuje problematyka błędu, a konkretnie kwestia, czy maszynę można wprowadzić w błąd. Wielu jest zwolenników personifikacji komputera, którzy pracę maszyny porównują do czynności wykonywanych przez osobę. Następnie odpowiedź na pytanie, czy w danym przypadku miała miejsce czynność oszukańcza, otrzymują oni w oparciu o stwierdzenie, czy w danym konkretnym wypadku znajdująca się na miejscu komputera istota ludzka również zostałaby zwiedziona przez sprawcę. Metoda ta budzi jednak pewne zastrzeżenia jako zbyt spekulatywna i niejasna[27]. Zgodnie z innym spojrzeniem na to zagadnienie w przypadku komputera można mówić o czynności oszukańczej wtedy, gdy sprawca, działając bez upoważnienia, „zataja" ten fakt przed urządzeniem przetwarzającym dane. To pozwala uniknąć rozważań związanych z przebiegiem procesu decyzyjnego w przypadku komputera lub też wzorca osoby. Minusem tej koncepcji jest to, że komputery nie zawsze są zaprogramowane w ten sposób, aby sprawdzać bądź też zapytywać o upoważnienie.

---

[25] S. Frey, op.cit., s. 182.

[26] Ibidem, s. 182.

[27] G. Zahn, *Die Betrugsähnlichkeit des Computerbetrugs (§ 263a StGB)*, Aachen 2000, s. 188.

W związku z tym wysunięto propozycję, by stosowanie przepisu § 263a StGB ograniczyć jedynie do sytuacji, gdy dochodzi do nadużycia w systemach, w których dokonywana jest taka kontrola[28]. W praktyce oznaczałoby to jednak znaczne zawężenie zakresu penalizacji regulacji oszustwa komputerowego.

Polska doktryna nie poszła tak daleko w analizie związku między art. 286 a 287 k.k. Zauważa się jednak, że rozgraniczenie między tymi dwiema regulacjami nastręcza wiele trudności organom ścigania[29]. Wyznacznikiem powinien być tutaj zarówno podmiot oddziaływania sprawcy, jak i wprowadzenie w błąd. W konstrukcji tradycyjnego typu przestępstwa podmiotem oddziaływania sprawcy jest osoba przez niego oszukiwana. Zazwyczaj jest ona przy tym również osobą pokrzywdzoną, ale nie jest to konieczne. Jest bowiem możliwa sytuacja, że osoba oszukiwana nie posiada żadnych praw do mienia, którym rozporządza. Przykładem może być tu wprowadzony w błąd listonosz wręczający sprawcy pieniądze przeznaczone dla kogoś innego[30]. Inaczej sprawa przedstawia się w przypadku oszustwa komputerowego. Tutaj nie występuje element wprowadzenia innej osoby w błąd bądź też wykorzystania tego błędu[31]. Bezpośrednim przedmiotem oddziaływania sprawcy jest bowiem nie osoba pokrzywdzona, lecz urządzenie lub system komputerowy[32]. Dla określenia relacji występujących między sprawcą, „wprowadzonym w błąd" komputerem a poszkodowanym doktryna niemiecka stworzyła pojęcie „trójkątnego oszustwa" (*Dreiecksbetrug*). Z jednej strony występuje bowiem sprawca, z drugiej komputer wykonujący program, a z trzeciej osoba poszkodowana (np. klient banku)[33]. Autorzy niemieccy nie wykluczają jednak sytuacji, w której sprawca oddziałuje na poszkodowanego wtedy, gdy ten drugi jest jednocześnie osobą obsługującą komputer. Zgodnie z wyrażanym w piśmien-

---

[28] Ibidem, s. 192.

[29] Por. A. Adamski, *Oszustwo komputerowe*, s. 15.

[30] B. Michalski, *Komentarz*, [w:] *KK – Część szczególna*, red. A. Wąsek, t. II, Warszawa 2005, s. 945.

[31] A. Adamski, *Prawo karne komputerowe*, Warszawa 2000, s. 115.

[32] R. Korczyński, R. Koszut, op.cit., s. 20.

[33] F. Haft, *Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität*, Neue Zeitung für Strafrecht 1987, z. 1, s. 8.

nictwie poglądem konstrukcja przestępstwa komputerowego przypomina w takim wypadku konstrukcję przestępstwa oszustwa klasycznego[34]. Odmiennego zdania są autorzy polscy, którzy w momencie, gdy czyn sprawcy skierowany jest nie tylko na mienie, ale również osobę, opowiadają się za zastosowaniem regulacji oszustwa klasycznego[35]. Brak oddziaływania przez sprawcę na proces decyzyjny poszkodowanego uważa się wręcz za element konstytutywny znamion przestępstwa oszustwa komputerowego[36].

Zarówno w polskiej, jak i w niemieckiej regulacji warunkiem koniecznym dla zaistnienia klasycznego oszustwa jest błąd, w wyniku którego dochodzi do rozporządzenia mieniem. Artykuł 286 k.k. przewiduje wprowadzenie w błąd (sytuacja, gdy w wyniku podstępnych działań sprawcy osoba ma mylne wyobrażenie o rzeczywistym stanie rzeczy) i wyzyskanie błędu (niezgodne z rzeczywistością opinie lub wyobrażenia osoby już istnieją, a sprawca jedynie je wykorzystuje)[37]. W § 263a StGB jest natomiast mowa o podstępnym wprowadzeniu w błąd oraz o zniekształceniu lub zatajeniu prawdziwych faktów i przez to wywołaniu błędu albo utwierdzeniu w nim osoby dokonującej rozporządzenia majątkowego. Generalnie rzecz biorąc, za błąd przyjęło się uważać rozbieżność między rzeczywistym stanem rzeczy a pewnym wyobrażeniem o tej rzeczywistości. Nie jest przy tym istotne, w jaki sposób sprawca będzie inną osobę w błąd wprowadzać (słowem, pismem, gestem czy też przez działanie albo zaniechanie)[38]. Istnieje jednak zgodność, że dotyczyć on musi okoliczności istotnych, czyli związanych z dokonywanym następnie przez osobę oszukaną rozporządzeniem mieniem lub też z faktem, że rozporządzenie mieniem jest dla tej osoby niekorzystne[39]. Na początkowym etapie rozwoju technologii informatycznych regulacja „klasycznego" oszustwa wciąż mogła spełniać swoją

---

[34] Ibidem, s. 8; H. Scheffler, op.cit., s. 222.

[35] A. Adamski, *Prawo karne komputerowe*, op.cit., s. 116; Michalski, op.cit., s. 982.

[36] P. Kardas, op.cit., s. 52.

[37] B. Michalski, op.cit., s. 946.

[38] Ibidem, s. 947 i 949.

[39] Ibidem, s. 948; S. Frey, op.cit., s. 248.

funkcję. Urządzenia przetwarzające dane były wtedy o wiele mniej skomplikowane i wpływanie na przebieg tego procesu mogło stanowić co najwyżej etap pośredni między wprowadzającym w błąd sprawcą a oszukiwanym człowiekiem obsługującym urządzenie, od którego decyzji zależało, czy nastąpi przesunięcie majątkowe, czy też nie[40]. Obecnie sytuacje, gdy w proces przetwarzania danych włączony jest jeszcze element ludzki, są już rzadkie. Uzależnianie zatwierdzenia wyników tymczasowych/pośrednich (*das Zwischenergebnis*) od ludzkiego procesu decyzyjnego byłoby zbyt czasochłonne[41]. W dzisiejszych czasach komputery są o wiele bardziej „samodzielne". Ta sytuacja stwarza jednak pewne problemy w procesie stosowania regulacji oszustwa „klasycznego". Wątpliwości powstały właśnie na gruncie pojęcia błędu. Zgodnie z poglądami większości doktryny wiąże się ono ściśle z pojęciem intelektu, jest więc stanem psychologicznym. To zaś sprawia, że jest ono nieadekwatne w przypadku komputera.

Oryginalne pojęcie „komputera pośredniczącego w błędzie" (*computervermittelter Irrtum*) sformułował F. Haft[42]. Zgodnie z tym autorem decydujące pytanie nie powinno brzmieć, czy w błąd można wprowadzić komputer, ale czy można wprowadzić w błąd człowieka za pośrednictwem komputera. Przede wszystkim automatyczne przetwarzanie danych nie może być postrzegane jako techniczna ciekawostka, ale jako coś, co doprowadziło do gruntownych zmian w ludzkim procesie decyzyjnym. Od automatów starego typu komputer różni się przede wszystkim tym, że w wyniku podziału pracy między nim a człowiekiem maszyna ta przejmuje pewne procesy decyzyjne. Inny autor (Müller-Lutz) podobnie postrzega relacje człowiek–maszyna. Podczas gdy zwykłe maszyny biurowe, pracując razem (jednocześnie) z człowiekiem, jedynie pomagają mu w wykonywaniu pewnych czynności, urządzenia automatycznie przetwarzające dane idą krok dalej. Między nimi a człowiekiem istnieje rzeczywisty podział pracy – człowiek tworzy programy, zgodnie z którymi takie urządzenie później samodzielnie i w odrębnej prze-

---

40 S. Frey, op.cit., s. 118.

41 Ibidem, s. 119.

42 Ibidem, s. 121–125.

strzeni czasowej wykonuje postawione przed nim zadania[43]. Na podstawie tych obserwacji F. Haft doszedł również do wniosku, że obecnie postrzeganie myślenia jako procesu czysto psychologicznego jest już nieadekwatne, ponieważ od momentu wprowadzenia komputerów przestało być ono przywilejem jednostki. W dzisiejszych czasach, przy takim podziale pracy jak opisany powyżej, myślenie charakteryzuje też zorganizowane grupy, w których człowiek i maszyna współpracują ze sobą. Przez takie rozumienie zjawiska informatyzacji życia można rozszerzyć stosowanie regulacji oszustwa klasycznego – mimo iż sprawca oddziałuje na maszynę, to kategorię błędu można odnieść do człowieka dzielącego z nią pracę. Na zarzuty, że w dużych przedsiębiorstwach, których pracownicy korzystają z pomocy komputerów, bardzo trudno jest wskazać konkretną osobę oszukaną za pośrednictwem danej maszyny, F. Haft odpowiada, że nie jest to istotne. W rzeczywistości bowiem komputer pracuje jedynie wtedy, gdy człowiek go zaprogramuje, wprowadzi dane itp. Dlatego element ludzki (chodź w coraz bardziej ograniczonym stopniu) jest z pracą takiej maszyny nieodłącznie związany. Koncepcja ta spotkała się jednak z ostrą krytyką ze strony doktryny. Zarzucano jej, że brak w niej konkretnie określonej osoby oszukanej oraz błędnego wyobrażenia, które są integralnym elementami konstrukcji oszustwa klasycznego.

Ponieważ próby pogodzenia pojęcia błędu z rzeczywistością związaną z rozwojem technologii informatycznych nie powiodły się, a w najlepszym razie wywołały wiele kontrowersji, konieczne stało się podjęcie działań legislacyjnych w celu zmiany tego stanu rzeczy. Zamiast stworzyć znamię analogiczne do pojęcia błędu, ale odpowiadające procesom zachodzącym podczas automatycznego przetwarzania danych, zrezygnowano z niego całkowicie. Nie przyjęła się tym samym propozycja użycia znamienia wprowadzenia błędu w informacji podanej urządzeniu technicznemu (*die Fehlinformation eines technischen Gerätes*)[44]. Jako odpowiednik „wprowadzenia w błąd" i „rozporządzenia mieniem" sformułowano natomiast zwrot „doprowadza do powstania szkody w mieniu innej osoby przez to,

---

[43] Ibidem, s. 122.

[44] F. Haft, op.cit., s. 8.

że wpływa na rezultat procesu przetwarzania danych". Zgodnie z założeniami prawodawcy proces przetwarzania danych ma odpowiadać ludzkiemu procesowi myślowemu lub decyzyjnemu. Natomiast wpływanie przez sprawcę na ten proces, za pomocą środków określonych w znamionach strony przedmiotowej, w przypadku komputera ma stanowić wprowadzenie w błąd, o ile następstwem takiego postępowania jest fałszywy wynik owego procesu[45].

Nie da się zaprzeczyć, że przestępstwo oszustwa komputerowego jest w pewien sposób powiązane z regulacją oszustwa klasycznego. W przypadku wątpliwości, czy w danej sytuacji powinien być zastosowany pierwszy, czy drugi typ przestępstwa, należy zwrócić szczególną uwagę na to, czy w danym przypadku czyn sprawcy skierowany był nie tylko przeciwko mieniu, ale też osobie (oszustwo klasyczne)[46]. Trzeba więc ustalić, czy miało miejsce „wprowadzenie w błąd" maszyny (oszustwo komputerowe), czy też oszukano człowieka[47].

Materialny lub formalny charakter przestępstwa oszustwa komputerowego

Kwestia, czy oszustwo komputerowe jest przestępstwem materialnym, czy formalnym, wywołała żywe dyskusje w polskiej doktrynie (sformułowanie przepisu § 263a StGB nie pozostawia żadnych wątpliwości co do jego materialnego charakteru – czyn zostaje dokonany w momencie powstania szkody[48]). Autorzy opowiadający się za tą drugą koncepcją[49] wskazują, że brak jest w znamionach ustawowych regulacji art. 287 k.k. skutku w postaci niekorzystnego rozporządzenia mieniem. Skutek taki natomiast stanowi o bycie przestępstwa oszustwa „klasycznego", które tym samym uznawane jest za przestępstwo materialne. Zaznacza się, że istotą przestępstwa z art. 287 k.k. jest usiłowanie uzyskania korzyści lub spowo-

[45] S. Frey, op.cit., s. 179.
[46] B. Michalski, op.cit., s. 982.
[47] S. Frey, op.cit., s. 209.
[48] H. Scheffler, op.cit., s. 227.
[49] A. Adamski, R. Korczyński, R. Koszut.

dowania szkody. Ma to ułatwić dochodzenie w toku procesu karnego[50]. Co więcej, gdyby przychylić się do tezy stanowiącej o materialnym charakterze tego przestępstwa, wszelkie zachowania sprawcy zmierzające do osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody, a niewywołujące zmian w świecie zewnętrznym, mogłyby być karane jedynie jako usiłowanie popełnienia przestępstwa oszustwa komputerowego[51].

Równie częsty jest w literaturze pogląd o materialnym charakterze regulacji art. 287 k.k. Powoływany jest argument, że dla realizacji znamion tego przestępstwa nie wystarczy samo tylko zachowanie się sprawcy, ale też zaistnienie skutków tego zachowania[52]. Ma to wynikać z konstrukcji znamion przestępstwa, które charakteryzują czyn poprzez tzw. czynnościowe określenie skutku. Według zwolenników tego poglądu już same czasowniki zastosowane przez ustawodawcę do określenia znamion przestępstwa komputerowego warunkują zaistnienie skutku. Podobna sytuacja ma miejsce w przypadku innych przestępstw materialnych, gdzie w znamionach występuje słowo „powoduje".

Mieszane stanowisko prezentuje B. Michalski[53], który dzieli regulację art. 287 k.k. na dwie odmiany. Pierwsza z nich polega na wpływaniu na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych i ma mieć charakter formalny. Autor argumentuje, że warunkiem popełnienia czynu zabronionego w tym przypadku jest zaledwie „wpływanie" na wymienione procesy, a nie spowodowanie ich faktycznych zakłóceń. Natomiast w wariancie polegającym na zmianie, usunięciu albo wprowadzeniu nowego zapisu danych informatycznych widzi on typ przestępstwa o charakterze materialnym, gdyż zmiana, usunięcie albo wprowadzenie nowego zapisu jest wymagalnym skutkiem. Jest to stanowisko

---

[50] K. Buchała, *Reforma polskiego prawa karnego materialnego*, [w:] *Prawne aspekty nadużyć popełnianych z wykorzystaniem nowoczesnych technologii przetwarzania informacji. Materiały z konferencji naukowej (Poznań, 20–22 kwietnia 1994)*, red. A. Adamski, Toruń 1994, s. 136; A. Adamski, *Prawo karne komputerowe*, s. 116.

[51] R. Korczyński, R. Koszut, op.cit., s. 35.

[52] P. Kardas, op.cit., s. 71.

[53] B. Michalski, op.cit., s. 988.

niespotykane dotychczas w doktrynie, gdzie nie wyróżnia się przestępstw o mieszanym, skutkowo-bezskutkowym charakterze. Nie wydaje się ono trafne z uwagi chociażby na niemożność określenia w takiej sytuacji konkretnego momentu popełnienia przestępstwa i – co za tym idzie – początku biegu terminu jego przedawnienia.

Analizując to zagadnienie, należy wpierw odnieść się do samej istoty przestępstw materialnych i formalnych. Za przestępstwa materialne (skutkowe) uważa się takie, których znamiona ustawowe wymagają, aby sprawca swoim działaniem lub zaniechaniem wywołał określony skutek. Dopóki tego skutku nie ma, dopóty czyn stanowi usiłowanie popełnienia przestępstwa. Przestępstwami formalnymi natomiast są te, dla których bytu skutek nie jest istotny, natomiast penalizowane jest samo zachowanie sprawcy. Należy dodać, że przez skutek zachowań sprawcy rozumie się zmiany nimi wywołane[54].

Przede wszystkim należy zauważyć, że dobrem chronionym przez przepis art. 287 k.k. jest mienie. Jednak dla bytu przestępstwa oszustwa komputerowego nie jest wymagane, aby nastąpił skutek w postaci przesunięcia majątkowego. Wystarczy już samo zachowanie się sprawcy, polegające na zmianie, usunięciu albo wprowadzaniu nowego zapisu danych informatycznych. Rzeczywiście, zastosowanie takich znamion czasownikowych, jak „usuwa" oraz „wprowadza", zdaje się implikować zaistnienie pewnego skutku. Trzeba jednak zaznaczyć, że czasowniki te służą jedynie określeniu zachowania sprawcy, które jest karalne. Przestępstwo oszustwa komputerowego charakteryzuje się penalizacją na przedpolu chronionego dobra[55] i w swojej istocie polega na usiłowaniu uzyskania korzyści lub spowodowania szkody[56]. Dlatego należy uznać je za przestępstwo formalne. Taka konstrukcja, prócz sporów w doktrynie, jest również przyczyną wątpliwości interpretacyjnych organów stosujących prawo[57].

---

54 A. Marek, *Prawo karne*, Warszawa 2003, s. 119.

55 Por. ibidem, s. 120.

56 Por. K. Buchała, op.cit., s. 136.

57 Por. A. Adamski, *Oszustwo komputerowe*, op.cit., s. 15.

Podsumowując, należy zauważyć, że regulacje oszustwa komputerowego zarówno w polskim, jak i w niemieckim prawie karnym są do siebie bardzo podobne. Częściowo tłumaczy to geneza obu regulacji. Szybkie wprowadzenie w Niemczech regulacji penalizującej ten typ przestępstwa sprawiło, że kraj ten brał aktywny udział w tworzeniu analogicznych uregulowań na płaszczyźnie międzynarodowej. Te z kolei były następnie recypowane w niewiele zmienionej formie przez polskiego ustawodawcę. Tym, co art. 287 k.k. i § 263a StGB mają wspólnego, jest z pewnością sprawiające trudności w ich stosowaniu podobieństwo do oszustwa „klasycznego". Również czynności wykonawcze w obu przepisach, mimo że literalnie sformułowane w sposób odmienny, są do siebie zbliżone na płaszczyźnie znaczeniowej, gdyż penalizują analogiczne zjawiska. Wszystko to sprawia, że ich porównywanie jest jak najbardziej uzasadnione.

Zusammenfassungen

Der Computerbetrug im polnischen und deutschen Strafgesetzbuch

Die Einführung des Computerbetrugs als eine neue Straftat in das polnische Strafrechtsystem fand erst in 1997 statt. Die entsprechende Regulation ist hingegen für den deutschen Gesetzgeber nicht neu. Man hat schon in den siebziger Jahren eine Gesetzlücke in diesem Land bemerkt, die eine Folge der Entwicklung der neuen Technologien war. Es hat sich nämlich herausgestellt, dass die bisherige Konzeption des Irrtums der Herausforderungen der informatisierten Welt nicht entsprach. Da die Bundesrepublik ein der ersten Ländern war, in denen die Computerstraftaten pönalisiert wurden, hatte das deutsche Recht einen großen Einfluss auch auf die internationalen Rechtstandarten. In Folge dessen hat die deutsche Konstruktion des Computerbetruges das polnische Recht stark beeinflusst. Der Tatbestand dieser Straftat ist zwar in beiden Strafgesetzbüchern anders bestimmt, fasst aber in beiden Ländern den gleichen Sachverhalt um und führt zu den ähnlichen praktischen Probleme bei dessen Anwendung. Als problematisch erweist sich besonders das Verhältnis zwischen dem Computerbetrug und dem „klassischen" Betrug und die Bestimmung des

Subjekts auf das der Täter des Computerbetrugs einwirkt. In dem polnischen Strafrecht ist es zusätzlich immer noch streitig, ob der Computerbetrug eine formelle, oder eine materielle Straftat ist.

Schlüsselwörte: Computerbetrug, Polnische Strafgesetzbuch, deutsche Strafgesetzbuch